

# STOP USING Google

Google makes billions by guzzling your personal data in order to show you targeted adverts. Loads of people are now switching to more private tools that also work better, smarter and faster.

**Jonathan Parkyn** tells you what to do

**G**oogle's unofficial motto 'don't be evil' became the company's mission statement in 2000. Those well-intentioned words appeared prominently in the company's official code of conduct (which you can still read on the Wayback Machine site at [www.snipca.com/37022](http://www.snipca.com/37022)). Tellingly, from around 2018 Google started erasing all reference to the phrase. Perhaps it

belatedly realised it could no longer get away with this sort of hypocrisy given some of its dubious practices.

To be clear, we think the tech giant has produced a number of genuinely brilliant products and services – most of which are available for free – and the company continues to push technology into new and exciting areas, such as advanced robotics and artificial intelligence. However, Google's business model is increasingly leaving a sour taste.

While other companies have been struggling with the economic impact of the pandemic, Google casually raked in a staggering \$37.10bn (around £27bn) in revenue between July and September 2020 – a rise of more than £2bn from 2019. And how does it generate these vast sums of cash? Mostly by tracking your

activities across the web and in the real world to build a comprehensive profile of you then using your personal information to sell targeted advertising.

Google is constantly being challenged for its flagrant disregard for users' privacy. In December, it was fined a whopping €100m (£90m) by French watchdog CNIL for breaking the country's regulations on how it uses trackers. But Google seems reluctant to change its data-gathering ways, while at the same time forcing users to pay for services they said would be free forever (see Google Photos, page 53).

So, over the next few pages, we'll explain why you may want to ditch some of these Google services, and suggest alternative tools and services that won't play fast and loose with your privacy.

## GOOGLE TOOLS YOU CAN DITCH

- Ditch Google Search for DuckDuckGo
- Switch from Chrome to Brave
- Replace Gmail with ProtonMail
- Move from Maps to OSM





## STOP USING GOOGLE SEARCH

Google started as a search engine and is still easily the most popular search tool on the planet, taking a whopping 92 per cent of the global market share from November 2019 to November 2020 (for proof, visit <https://gs.statcounter.com> and click Search Market Share). Its nearest competitor, Microsoft's Bing, accounts for a paltry three per cent.

Biggest doesn't always mean best, of course. And, while Google does a great job of scouring the web for websites, it's also adept at collecting data about you every time you carry out a search. It tracks not only what you search for, but also any links you click and images or videos you view. It analyses your search patterns and keeps track of any adverts you show interest in.

One reason Google collects this data is to help it deliver more relevant results whenever you carry out a search. But the company also stores all this information along with your search history and uses it to build a detailed advertising profile of you, so that it can target you with personalised ads. This is how it makes most of its money.

### Switch to a private search engine

One way to minimise the amount you're being tracked when you use Google Search is to make sure you're not logged in with a Google account. Bear in mind this will also make your search results less relevant, and Google may still be able to track you via other identifying factors, such as your IP address.

A more effective way to avoid Google's tracking is to use a different search engine. We'd avoid switching to Bing, because this would just mean Microsoft is gathering your data rather than Google. The best alternative from a privacy point of view is DuckDuckGo ([www.duckduckgo.com](http://www.duckduckgo.com)), which won't track your activity, store your search history or share any of your personal information. Better yet, the service routes any links you click in a way that prevents your search terms being shared with other websites.

DuckDuckGo includes many of the handy features you find in Google Search – type a maths calculation or a currency conversion and it will instantly provide an answer, for example. But some features, such as instant translation to and from English, are absent.

And, because DuckDuckGo doesn't

gather data about you, your search results aren't always as relevant. On the upside, you won't ever be targeted by adverts.

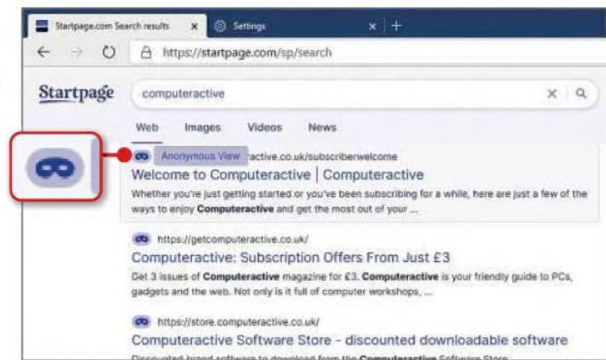
If you want the benefit of Google's high-quality search results without all that tracking and profiling, then you could try Startpage ([www.startpage.com](http://www.startpage.com)) – a search engine that pays Google a small fee to use its search technology, but doesn't record your search queries or use tracking and cookies that can identify you.

Like many free services, Startpage makes its money via advertising and sponsored links, but these adverts aren't generated by analysing your personal data. The result is a good balance between accuracy and privacy. Clicking the mask icon (see screenshot above) next to a link in the search results will take you to that site anonymously.

### Set your preferred search engine

Switching your search engine means setting an alternative provider as your browser's default. For example, if you're happy to stick with Google's web browser Chrome (see page 53, if you're not), you can replace Chrome's default search engine (Google) by clicking the menu button (three dots, top right), then Settings. Here you can select another search provider of your choice from the dropdown menu under 'Search engine' – DuckDuckGo is listed here, for instance.

If the search engine you want isn't listed, click 'Manage search engines', then Add. Type the name of the search engine you



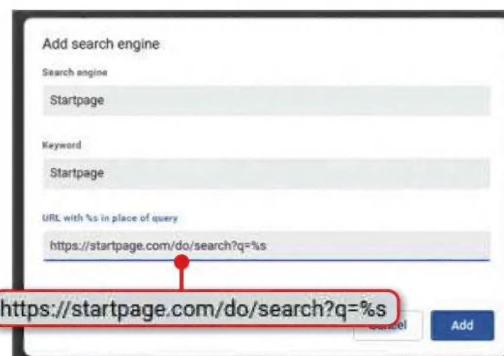
Startpage lets you view websites anonymously by clicking the mask icon next to a search result

want under both 'Search engine' and Keyword. Next, under URL, enter the search-results web address for the search engine you want, followed by %s – <https://www.startpage.com/do/search?q=%s>, for example. (For most search engines, their results URL ends after the equals sign, so %s after that, see screenshot below left). Click 'Add', then look for your new search engine in the list of 'Other search engines' – click the three-dots button next to it and select 'Make default'.

Microsoft's browser Edge has settings that work in much the same way, but to find them you need to click the menu button (three dots), Settings, 'Privacy, search, and services', then 'Address bar and search'. Some privacy-first browsers, such as Brave ([www.brave.com](http://www.brave.com), see page 52), let you select either DuckDuckGo or Startpage as your default search engine during the initial setup.

On a phone or tablet, changing your search engine works in a similar way. In Chrome for iOS and Android, for example, tap the menu button (three dots), tap Settings, then 'Search engine'. Here, you'll be able to select DuckDuckGo. Tap the Back button when you've finished. Similarly, in Edge, tap the three dots, Settings, then 'Advanced settings'. Tap 'Search engine', then Others to select DuckDuckGo. Finally, tap Done.

Other than Edge and Chrome, there aren't many mobile browsers that let you add more alternative search engines, meaning you may not be able to set Startpage as your default search engine. There is, however, a free, Startpage app ([www.snipca.com/36963](http://www.snipca.com/36963) for Android, [www.snipca.com/36964](http://www.snipca.com/36964) for iOS).



You can add search engines to Chrome by typing their search-results URL, followed by %s





## STOP USING GOOGLE CHROME

Chrome has been the world's most popular web browser since 2012, but there are two big reasons why you should consider ditching it: privacy and performance. Chrome provides Google with more ways to gather data about you by storing cookies, and if you sign into the browser with your Google account, the company records every site you visit. Chrome's privacy policy even admits "we use your browsing data to improve and personalise your experience within Chrome" – see [www.snipca.com/36977](http://www.snipca.com/36977).

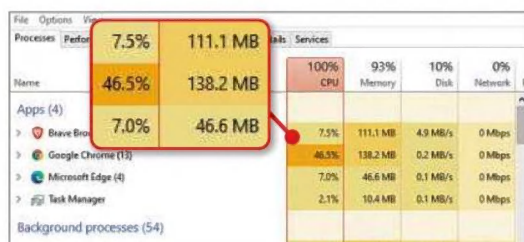
Chrome also offers little protection against third-party trackers – cookies placed on your computer by other websites that lets them track your movements around the web and, potentially, sell your browsing data to other organisations. Chrome allows these trackers by default and in a blog post in 2019 ([www.snipca.com/36979](http://www.snipca.com/36979)) Google admitted that it has no intention of blocking them.

You can disable third-party trackers in Chrome, but that brings us to another problem with Google's browser – its privacy settings (click the menu button, Settings, then 'Privacy and security') are unnecessarily complicated compared with many of its rivals, making it hard to know what to switch off.

We also don't like the way Chrome signs you up to send usage data back to Google before you've even downloaded it. It's easy enough to click the Download Chrome button on the [www.google.co.uk/chrome](http://www.google.co.uk/chrome) homepage without noticing the pre-ticked box that grants Google the power to gather even more information about you.

### Memory hog

One reason Chrome became so popular was that it was much faster than Internet Explorer, Opera and Firefox. These days, Chrome still feels fast, but it has a habit of putting an undue strain on your PC in the process. Our screenshot below shows



Google's Chrome browser tends to use more of your PC's memory than its rivals

Windows Task Manager with three different browsers – Chrome, Brave and Edge – running at the same time. All three have the same four tabs open, but you can see that Chrome is using up significantly more CPU (46.5%) and memory (138.2MB) resources than the other two.

This is partly due to how Chrome handles each tab as a separate process. Microsoft actually released a fix for the excessive memory usage in Chromium-based browsers – via the Windows 10 May 2020 Update ([www.snipca.com/36980](http://www.snipca.com/36980)). Annoyingly, Google is yet to make use of this fix for Chrome, so it remains a memory hog.

### Switch to a more private browser

If privacy is your overriding concern, consider switching to Mozilla's open-source browser Firefox ([www.snipca.com/36983](http://www.snipca.com/36983)), which by default stops websites gathering data on you by blocking third-party tracking cookies.

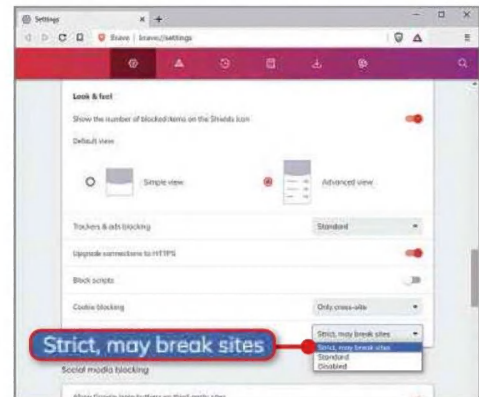
The Brave browser (<https://brave.com>) goes even further by preventing what's known as 'fingerprinting' – a process whereby sites build up a detailed profile of you based on 'semi-identifying' factors revealed by your browser, such as your PC's language setting, its hardware and so on.

Cleverly, Brave won't block websites that have a genuine reason to get this information (banking websites use it to detect suspicious login attempts, for example), however if you prefer you can enforce it on *all* sites by clicking the menu button, Settings, scrolling to the Shields section and selecting Strict from the 'Fingerprinting blocking' box (see screenshot above right).

### Get better performance

If a faster browser is your priority, Microsoft Edge is a safe bet (just make sure you're using the newer Chromium-based version: [www.snipca.com/36985](http://www.snipca.com/36985)). As explained earlier, Edge benefits from the memory-handling fix that Chrome lacks, meaning it takes up fewer system resources.

We also like Edge's privacy settings, which are much more straightforward than Chrome's. Under Settings,



Brave lets you block fingerprinting on all sites, but it may result in some sites not working properly

'Privacy, search, and services', there's a simple, three-tiered tracking prevention option. Balanced mode is selected by default, which blocks most trackers, but you can easily opt for Strict mode to maximise your privacy.

Chrome's slower performance is less of a problem on mobile devices but privacy remains a worry. Brave, Firefox and Edge all offer mobile apps you can try. We also recommend trying DuckDuckGo's Privacy Browser (Android [www.snipca.com/36981](http://www.snipca.com/36981); iOS [www.snipca.com/36982](http://www.snipca.com/36982)). As well as letting you run private searches, DuckDuckGo's browser automatically blocks third-party trackers, enforces HTTPS encryption on all websites, and lets you clean up all your browsing data instantly with one tap.

### Move to a new browser

Most rival web browsers let you import your bookmarks and other data from Chrome. Brave prompts you to do so during its setup process – simply select Chrome in the 'Import from' menu. In Edge, click the menu button, Settings, Profile, then select the 'Import browser data' option and select Google Chrome in the dropdown menu. Choose your profile, select the items you want to import, then click the Import button.

Mobile browsers don't always offer an easy way to import bookmarks and browser data from Chrome, but most are able to sync user data between mobile and desktop versions of the same browser. So, the simplest way to get your data on to your device is to import it from Chrome to the browser of your choice on your PC first, then sign into the mobile version of your new browser using the same account as your PC.



## STOP USING GOOGLE PHOTOS

Until recently, Google Photos offered free, unlimited online storage for all your photos and videos. You needed to use the 'High quality' option rather than Original (this compressed your photos to reduce their size, without noticeably affecting their quality), but this basically allowed you to back up your photos for free and sync them across all your devices, without using any of your 15GB Google storage allowance.

The service proved particularly popular with Android and iOS users, letting them automatically back up photos taken on their phones. Millions of PC users have also relied on the service, uploading the photos on their computers to Google's storage for free using the Backup and Sync tool ([www.snipca.com/36996](http://www.snipca.com/36996)).

In November last year, however, Google announced that it was making big changes to its Photos app ([www.snipca.com/36997](http://www.snipca.com/36997)). From 1 June 2021, any new photos or videos that you upload to Google Photos or Google Drive will count towards your free 15GB of storage, even if you opt for the 'High quality' setting.

Should you need more space (and you probably will, because the 15GB is shared across all Google services, including Gmail and Docs), you'll have to start paying a subscription, starting at £1.59 a month for 100GB storage. Photos you've already uploaded in 'High quality' are currently exempt from these changes and therefore won't count towards your quota.

However, Google has repeatedly shown

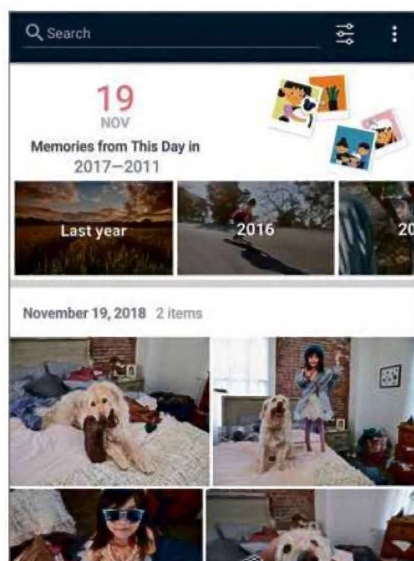
that it's willing to change its terms at relatively short notice. For this reason, we recommend you don't rely on the service as a long-term backup solution. Even more concerning is the fact that Google recently sent an email to users, threatening that if they exceed their online storage limit or leave their account inactive for two years, the company "may delete your content across Gmail, Drive and Photos".

If you have one of Google's Pixel phones, you won't have to worry about these changes. The company is allowing Pixel users to carry on using Google Photos with unlimited storage, as before. But it's also worth bearing in mind that photos you store in Google's online storage services fall under the company's Terms of Service (<https://policies.google.com/terms>), which state that Google has the right to "host, reproduce, distribute, communicate and use your content", including publicly displaying or modifying it. While that sounds terrifying, these permissions are required for many of the features within Google Photos (such as when you choose to create a sharing link for one of your images). However, if it still leaves you feeling uneasy, there are alternatives.

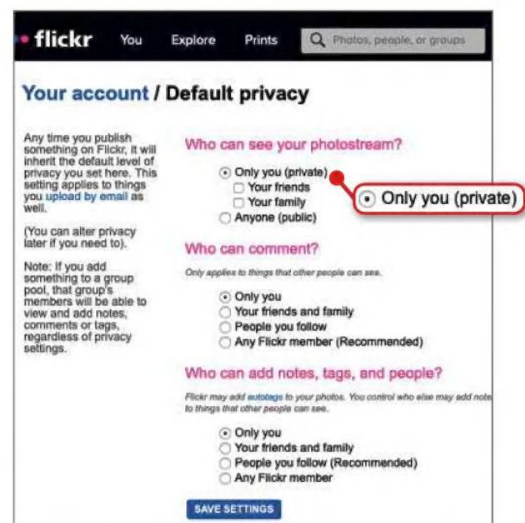
### Get unlimited storage elsewhere

Unfortunately, there isn't an obvious like-for-like alternative to Google Photos. There are other online storage services (see page 56), but none offer free unlimited photo storage and most lack the advanced features of Google Photos, such as photo editing, filters, scanning images for text or creating and sharing photo albums.

The next best thing is Amazon Photos ([www.snipca.com/36998](http://www.snipca.com/36998)), which offers some of Google Photos' capabilities, including family photo sharing and syncing across devices (see screenshot left). Indeed, some readers have already switched to it (see 'Why I stopped using', page 42). If you're an Amazon Prime subscriber, you also currently get unlimited full-resolution photo storage. Bear in mind that if you end your Prime subscription, you'll need to move your photos elsewhere or pay separately for the service (you get 5GB free, but beyond



Amazon Prime customers can store unlimited photos for no extra charge and enjoy similar features to Google Photos



If you use Flickr to store photos and don't want to share them, make sure you set them to be private

that prices start at £1.49 per month for 100GB).

Flickr ([www.flickr.com](http://www.flickr.com)) is another possibility. Although it drastically reduced its free storage from 1TB to just 1,000 photos late in 2018, its paid-for Flickr Pro plan is good value if you have thousands of photos. For £56 per year, you get unlimited storage - plus Flickr won't apply any compression to your photos. In comparison, Google charges £79.99 for 2TB of storage.

If you do decide to switch to Flickr, make sure you check your privacy settings, otherwise your photos may be visible publicly. Click your account icon, Settings, 'Privacy & Permissions', then click Edit next to 'Who will be able to see, comment on, add notes, or add people' and change the defaults to 'Only you (private)' - see screenshot above - or friends and family if you want to share with people you know.

### Move your photos offline

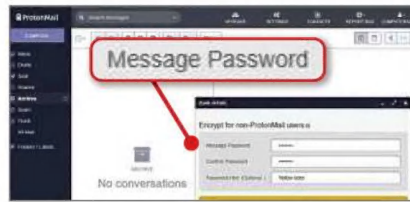
If privacy and preserving your photos are your main concerns, there's an argument for bypassing online-based services altogether and backing up via an external hard drive instead. It's not ideal, though, as hard drives are susceptible to damage and theft. We therefore recommend creating multiple backups and storing one somewhere other than your home. The good news is that you won't have to pay an ongoing subscription as you can just use the backup tools that are built into Windows 10 (found under Settings, 'Update & Security', then Backup).



## STOP USING GMAIL

Google has repeatedly come under fire for the way it handles Gmail users' data. It used to scan emails so it could add targeted advertising next to email messages. Google announced an end to this practice in 2017, but only a year later the *Wall Street Journal* revealed that the company had been allowing developers of third-party apps access to users' emails ([www.snipca.com/36999](http://www.snipca.com/36999)) and – worse still – that some messages had been read by staff members, not just automated software.

In addition, some of Gmail's features (such as Smart Compose, which suggests words when you're writing an email) rely on algorithms to scan the contents of your emails. Google used to opt you into these features automatically, but you may have recently seen a notice when logging into Gmail, asking you whether you want to continue using what it calls 'smart features' (essentially an admission by Google that it probably shouldn't have



**ProtonMail lets you send password-protected messages to non-ProtonMail users**

opted you in without consent in the first place – see page 11, Issue 596).

### End-to-end encrypted mail

If security and privacy concerns are turning you away from Gmail, ProtonMail (<https://protonmail.com>) could be the ideal solution. Like Gmail, ProtonMail can be accessed via a web browser or via Android ([www.snipca.com/37001](http://www.snipca.com/37001)) and iOS ([www.snipca.com/37002](http://www.snipca.com/37002)) apps.

Unlike Gmail, however, the company's servers are based in Switzerland, meaning that all user data is protected by

strict Swiss privacy laws. ProtonMail will never track your IP address and you can even sign up for an account anonymously.

In addition, when you email other ProtonMail users your messages are end-to-end encrypted (E2EE), meaning no other person or program can read them except you and the recipient (though read 'Question of the Fortnight', page 10, for how this might change). You can also send encrypted emails to non-ProtonMail users by securing them with a password (see screenshot). It's a bit complicated as you need to send them the password separately (such as via a WhatsApp message), but useful for occasional use – for example, if you need to email banking details to someone.

There are some downsides to ProtonMail. The free service limits you to 500MB of storage and 150 messages a day (which might not be enough for businesses). For £3.60 a month you get 5GB of storage and 1,000 messages a day.

## STOP USING GOOGLE MAPS

It's one thing having Google following you around the web, but stalking you wherever you go in real life is just downright creepy. If you have the Google Maps app installed on your phone or tablet, however, you are effectively allowing Google to track your every move.

Google says it collects your location data so that it can improve its services and provide you with personalised content, such as the location of nearby restaurants. And it's certainly true that, without access to your location data, much of what makes Google Maps so useful just wouldn't work.

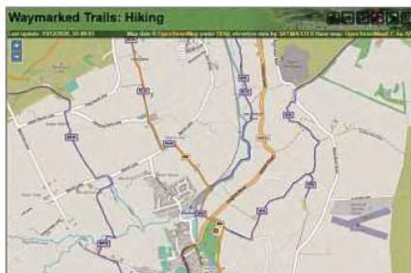
However, dig into Google's Privacy & Terms document ([www.snipca.com/37003](http://www.snipca.com/37003)), and you'll discover that the

company also uses your location to send you targeted adverts. On top of that, by default, Google Maps saves a record of everywhere you go with your devices, even when you're not actively using a Google service.

You can view a record of precisely when and where you've been tracked by logging into [www.snipca.com/37004](http://www.snipca.com/37004) with your Google account. Click the dustbin icon at the bottom-right of the map to delete your location history.

### Open-source mapping

Most map and navigation services require access to your location in order to function, but there are some that respect your privacy and don't constantly record your movements. OpenStreetMap (OSM, [www.openstreetmap.org](http://www.openstreetmap.org)) doesn't use your location data to target you with ads, nor will it share your information with third parties. Instead, it's an open-source mapping service that includes data collected by volunteers the world over. It's also used by other services to provide all sorts of mapping information, such as Waymarked Trails ([www.waymarkedtrails.org](http://www.waymarkedtrails.org)), which overlays OSM maps with walking, cycling and other routes created by users (see screenshot left).

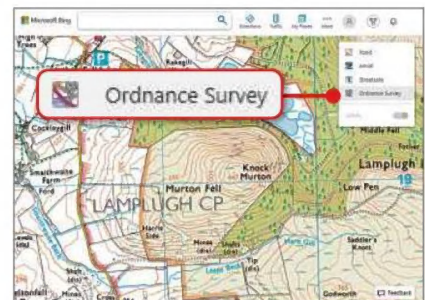


**Waymarked Trails uses OSM maps to display walking routes (shown here in purple and orange) and more**

On your phone or tablet, you can try OsmAnd (Android [www.snipca.com/37006](http://www.snipca.com/37006); iOS [www.snipca.com/37007](http://www.snipca.com/37007)), which uses OSM's map data and adds useful extras such as GPS navigation, spoken instructions and offline maps.

### Get OS maps for free

If you want something with more detail, go to Microsoft's Bing Maps ([www.bing.com/maps](http://www.bing.com/maps)) to find some fabulous Ordnance Survey maps – simply click the Road box at the top right of the map, then select Ordnance Survey (see screenshot below). As you zoom into the map, the view will change from the Landranger (1:50k scale) to Explorer (1:25k) maps, letting you plan everything from a short country stroll to a weekend hike.



**Bing Maps gives you full access to OS Landranger and Explorer maps**





## STOP USING YOUTUBE

Did you know that YouTube is owned by Google? And did you also know that if you don't tighten up your settings, you could be letting total strangers know what you watch online? Sadly, YouTube shares the same lax attitude to personal privacy as Google's other services.

### Stop strangers seeing your favourite channels

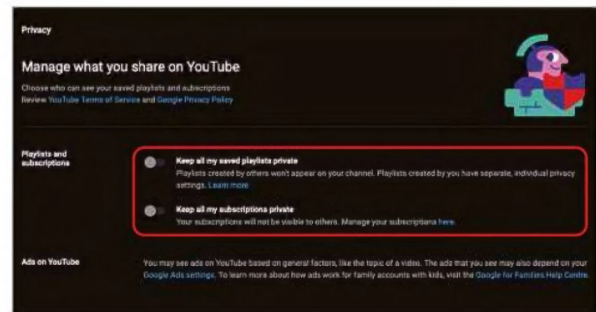
Until December 2019, for example, a list of your 'liked' videos (those you've clicked the thumbs-up icon for) was publicly viewable, meaning anyone could see them. Thankfully, YouTube now keeps that information private. But it's still possible for anyone to see which videos you've shown an interest in because YouTube allows visitors on to your channel to see which other channels you've subscribed to and which playlists you've added.

To disable this, you need to log into [www.youtube.com](http://www.youtube.com) then click your account icon (top right), select Settings, then click Privacy. Next to 'Playlists and

subscriptions', make sure both sliders are turned off (see screenshot right). Even if you disable these settings, YouTube will continue to target you with adverts, either based on your Google Ads settings or the content of the videos you're watching. And, of course, Google tracks your activity on YouTube, as it does with the company's other services.

### Sign out of Google when watching videos

It's tricky to recommend an alternative given that YouTube has the free video-streaming market virtually to itself. You could try Vimeo (<https://vimeo.com>), which doesn't sell your data to third parties. However, it *will* serve up targeted ads based on data it's collected about you,



Turn off these options to stop strangers seeing your favourite channels and playlists on YouTube

and its content is too niche for most tastes in any case. Sadly, there just isn't another service that offers the same variety as YouTube and it's probably unrealistic to stop using it altogether.

However, you can stop Google gathering data on you by not signing into your account when watching videos. To do this, click your account icon and select 'Sign out'. Bear in mind this will turn off many of YouTube's features, including saving videos for later and posting comments.



## STOP USING GOOGLE DRIVE AND DOCS

Google Drive remains one of the more generous online-storage services, offering 15GB for free, compared with 5GB for Microsoft OneDrive and just 2GB for Dropbox. But, as we've already seen (on page 53), Google is changing its online-storage policy and it could conceivably end up reducing its free allowance, as Microsoft did in 2015.

There's a popular myth that claims Google takes legal ownership of anything you store on Google Drive, but that's actually not true. As stated in Google's Terms of Service, you "retain ownership of any intellectual property rights that you hold in that content".

However, as we mentioned on page 53, Google's Terms of Service (<https://policies.google.com/terms>) lets it effectively do what it likes with any files you store online. And, in Google Drive's Additional Terms of Service ([www.snipca.com/37015](http://www.snipca.com/37015)), you'll see that Google retains the right to review and remove content, should it see fit, which essentially means it can open your files and read or scan your documents if it wants to, and delete anything it doesn't like.

Google Drive is inextricably linked to Google's online office suite, which

includes **web apps** such as Google Docs and Sheets, as well as tools for collaboration. You might therefore assume the most obvious alternative is Microsoft's OneDrive (<https://onedrive.live.com>), which provides access to Microsoft's online versions of Word, Excel and so on, as let you collaborate online with others.

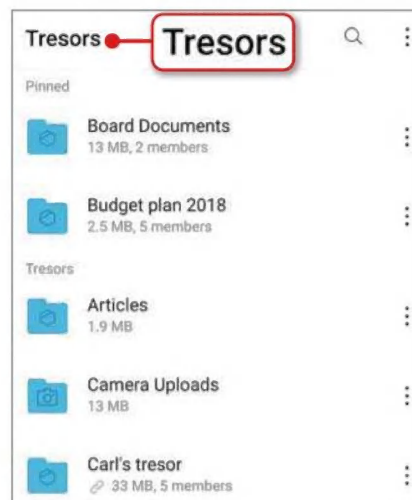
However, as we pointed out earlier, you get less free storage than Google, and its

privacy policy ([www.snipca.com/37016](http://www.snipca.com/37016)) isn't much more reassuring than Google's, giving Microsoft the right to "collect data about your usage of the service, as well as the content you store".

### Switch to encrypted file storage

For files that you don't want anyone seeing or analysing for data, we'd suggest using an online storage service that offers end-to-end encryption, such as Tresorit, available for Windows, Android and iOS (<https://tresorit.com/download>). Tresorit is another Swiss firm that provides **zero-knowledge authentication**, meaning it's unable to access your content. Once you sign up, you can store your files in encrypted folders called Tresors (see screenshot left).

There are some drawbacks. Firstly, Tresorit's free storage is capped at just 3GB – it costs £6.67 per month to expand this to 500GB. Also, Tresorit doesn't include a built-in office suite, so you'll need to provide your own word processor, spreadsheet tools and so on. Using an offline office suite in this case, such as LibreOffice (free from [www.libreoffice.org](http://www.libreoffice.org)), will help to keep your files private and secure.



Tresorit lets you save your files in encrypted folders that it's unable to access





## STOP USING GOOGLE CALENDAR

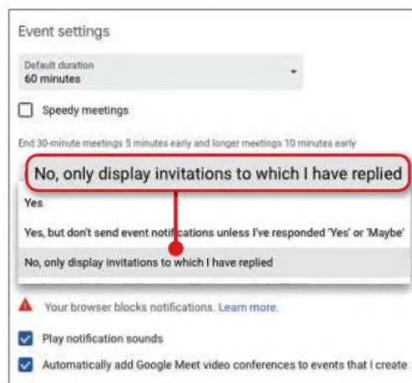
There's nothing particularly insidious about Google Calendar, but it is closely connected to Gmail – to the extent that Gmail will automatically add events to your calendar if it detects emails confirming events like upcoming flights or hotel reservations. Some find this clever and convenient; others creepy and intrusive. It also has the unwanted side effect of letting spam show up in your calendar – including invitations from strangers for video chats.

You can plug these holes by logging in at <https://calendar.google.com>, then clicking the cog icon and selecting Settings. Next, on the left, click 'Event settings' and select 'No, only display invitations to which I have replied' (see screenshot below) from the 'Automatically add invitations' dropdown menu.

Next, untick 'Show declined events' under 'View options' and untick 'Automatically add events from Gmail to my calendar' below 'Events from Google'. However, if you're giving up Gmail and other Google services, it makes sense to also switch from Google Calendar.

### Switch to Microsoft Calendar or ProtonCalendar

There are plenty of alternative calendar tools, but probably the most convenient is Windows 10's built-in Calendar app.



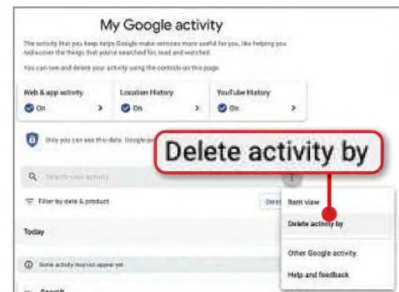
Select this option so Calendar only shows invitations for events that you've responded to

## Download & delete your Google data

As we've explained, Google stores a huge amount of your personal data. Google Takeout provides a way to get this information back, whether you're moving to a different service or simply want to download and keep a copy of it.

Sign in with your Google account at <https://takeout.google.com> and browse the categories. By default, all 50-plus categories are pre-ticked, meaning they'll all be included in your data download, but you can untick any you don't want.

Click the 'Next step' button when you're ready, then select your delivery method – 'Send download link via email' is probably the easiest for most people. Under 'Frequency', select 'Export once' (alternatively, choose a recurring download every two months). Leave the file type as .zip and select the file size for your download file – you can opt to split the ZIP file into chunks of between 1GB and 50GB in size, if that's more



Select 'Delete activity by' to remove all your data from Google's servers

convenient. Click the 'Create export' button to finish.

If you want to delete all the data Google has stored on you, sign in at <https://myactivity.google.com> and either scroll through and choose what to erase, or click the three dots to the right of the search box and select 'Delete activity by' (see screenshot). Finally, click Always and follow the remaining steps.

While many other calendar apps are aimed at business users, Microsoft's Calendar is firmly geared towards home users and is fully integrated into Windows 10, meaning you can see events in Live Tiles in the Start menu, receive notifications and more. Better still, if you're signed into Windows with a Microsoft account, your calendar is automatically synced across all Windows 10 devices you're signed into, as well as in Outlook.com and through the Outlook app on mobile devices.

For greater privacy, consider ProtonCalendar. It's created by the same developers as ProtonMail and offers similar levels of protection, including end-to-end encryption, no trackers, and no data sharing with third parties. The only caveat is that it's still in beta ([www.snipca.com/37017](http://www.snipca.com/37017)) and currently

available only to paying ProtonMail users. However, Proton has promised to make it free soon.

First, you need to export your data from Google Calendar. To do this, log in at <https://calendar.google.com>, click the cog icon, Settings, then 'Import & export' on the left. Click the Export button and save the ZIP file to your PC. Extract its contents and you should see an '.ics' file for each calendar you've been using in Google Calendar. If you're switching to Windows 10's calendar, double-click each '.ics' file in turn – the Calendar app will now launch. Select the Windows calendar you want to add your Google Calendar events to, then click 'Add to calendar'. If you opt for another calendar, you should be able to import the '.ics' file – just check for import options in the tool's settings. **ca**

**NEXT ISSUE** On sale Wednesday 27 January

## Should you get a... TV BOX OR TV STICK?

What's best for you – a set-top box for recording, or a stick for streaming? We'll tell you



**PLUS**

- Every Windows tool that will disappear soon And what to use instead
- Run Malwarebytes with your antivirus Double protection, no clashing

**ONSALE  
Weds  
27  
Jan**

Subscribe to Computeractive at [www.getcomputeractive.co.uk](http://www.getcomputeractive.co.uk)